

[Click here to print](#)

## Clouded in uncertainty - the legal pitfalls of cloud computing

### For some companies the legal risks of using cloud-based services can far outweigh the business benefits

John Salmon, [Computing](#) 24 Sep 2008

Business leaders are becoming more open to the idea of buying IT as a service, rather than owning infrastructure. The enticing prospect of releasing the enterprise from the shackles of buying and maintaining hardware and from the hassle of software licensing and support, has fuelled interest in cloud computing. But such momentous changes also carry some risks.

#### What is cloud computing?

Cloud computing describes the use of software, storage or processing services delivered over the web from massive datacentres. Google Apps is an example it provides email, word processing and spreadsheet applications to any computer with a browser and an internet connection. All other software and data sits on Google's servers.

Various terms have been used for cloud computing or aspects of it over the years remote computing, application service providers, software on demand, software-as-a-service, utility computing and web services. The terminology has evolved but the legal principles are the same.

For most users the main benefit of cloud computing will be cost. It can offer savings on hardware, software licensing fees and support.

#### What terms and conditions can I expect to see in a cloud computing licence?

Typically the customer will be required to agree to the provider's standard terms of service without any scope for negotiation. The terms are likely to be biased in the provider's favour.

For example, the terms of service for Amazon Web Services state: "Neither we nor any of our licensors shall be liable to you for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to damage for loss of profits, goodwill, use, data or other losses (even if we have been advised of the possibility of such damages) in connection with this agreement."

While the exclusion of indirect losses is typical in service contracts, the exclusion of direct losses is a risky position for any customer. If Amazon loses your data and that loss costs you money, Amazon is saying that you cannot do anything about it.

Such a clause may be challengeable as "unfair" under UK law, depending on the circumstances. When a business is the customer, rather than a consumer, it is harder to show that a contract term is unfair, because businesses have less protection than consumers. But it is harder still to challenge a contract that is based on US law in a US court another provision to be expected when contracting with a cloud computing provider from that country. That is not only because suing in the US is inconvenient and expensive, it is also because courts over there have an even lower expectation of fairness in business contracts.

## **Will there be any guaranteed service level?**

From a business perspective, having agreement on the service levels to be provided may seem vital in any IT contract. Incorporating the standard of performance required by the supplier as a contractual requirement provides the customer with a potential contractual remedy if the standard is not satisfied.

Amazon's Elastic Compute Cloud is a web service that provides "resizable compute capacity in the cloud". According to its description, it "allows you to obtain and configure capacity with minimal friction" and "reduces the time required to obtain and boot new server instances to minutes".

That may suggest that there is some sort of service level guarantee but there isn't. There are no remedies available if obtaining capacity causes great friction or booting a new server instance takes forever. There is no guaranteed up time in fact the contract says that Amazon shall not be responsible for any service interruptions.

It gets worse.

"We and our licensors do not warrant that the service offerings will function as described, will be uninterrupted or error free, or free of harmful components, or that the data you store within the service offerings will be secure or not otherwise lost or damaged," says Amazon.

In fact, the only right that the customer has is to terminate the service.

## **Will information I store in the cloud be secure?**

One would expect companies offering storage facilities in the cloud to have stringent security measures in place to protect its users' data. However, users of cloud computing will need to evaluate a service provider's offering to ensure it has security in place that is appropriate for the nature of the data stored. Data might be personal data or proprietary confidential information.

If you are a business holding personal data, the Data Protection Act (DPA) requires "appropriate technical and organisational measures" to be put in place to ensure the security of the data held. The obligation to maintain strict control over the security of personal data remains with the customer regardless of whether the personal data is held by a service provider on their behalf. In its capacity as a data controller the organisation that controls how and why personal data is processed a business must put in place processing contracts with any third party known as the data processor appointed to collect, store or destroy personal data on its behalf.

These processing contracts must be in writing and must set out what security measures should be taken to safeguard the data. The standard terms and conditions of cloud computing service providers, for example Salesforce.com, provide no guarantee as to the security of data. On the contrary, "Salesforce.com shall not be responsible or liable for the deletion, correction, destruction, damage, loss or failure to store any customer data".

UK businesses storing personal data with Salesforce.com on the basis of their standard terms and conditions could find themselves in breach of their security obligations under the Data Protection Act.

Financial firms subject to Financial Services Authority (FSA) regulation will also need to comply with the FSA's security requirements. The FSA in its 2008 report Data Security in Financial Services noted that "firms' dealings with third-party suppliers are a major concern" and "data security in financial services firms needs to be improved significantly". It may not be impressed with firms signing up to web services that lack any security guarantees.

The location of data is another issue for customers to consider. The DPA requires that personal data generally should not be transferred outside the European Economic Area (EEA) unless the country of destination ensures an adequate level of protection in relation to the personal data. There are solutions

available for transferring personal data out of the EEA, including the EU/US Safe Harbor Deal to which Salesforce, Google and Amazon are signed up.

Not many others have, though, and while Safe Harbor is not the only compliance solution for transferring personal data, you should check this issue with any US provider.

Customers should also be aware that if data is held on a server located in another country, law enforcement agencies may be able to access that data under local laws.

### **Is cloud computing right for your business?**

The attraction of cloud computing is evident for a small startup business lacking the finances to develop and maintain IT infrastructures in-house or to commission others to do so on its behalf. Customers looking for IT resources, for example, for only six months a year will also benefit from the pay-as-you-go approach without having to maintain a system that is not, or barely, being used for the other half of the year.

Companies with the finances and in-house technical abilities to develop their own systems should weigh up the cost benefits against the risks and consequences of having no recourse should any data they store be lost or accessed without their consent or if the service provider fails to live up to its service claims.

While the risks may seem remote with the large service providers, where customers are handling personal data the contractual terms and conditions alone would result in a breach of regulatory requirements. The Information Commissioner has this year been given powers to fine organisations that lose customer data, and has warned of substantial fines for the worst breaches of the DPA.

We have also seen the FSA more ready to issue fines for data breaches. In the past three years, the FSA has fined Norwich Union £1.26m, BNPP Private Bank £350,000, Nationwide £980,000 and Capita Financial Administrators £300,000 for failings relating to information security lapses and fraud.

For many organisations, the risks may simply outweigh the benefits.

*John Salmon is a partner at [law firm Pinsent Mason](#).*

© 2008 Incisive Media Investments Ltd

[Click here to print](#)

[Close this window](#)